Data Protection & Cybersecurity

Do you Need a Data Protection Officer?

Kherk Ying Chew
kherkying.chew@
wongpartners.com

Serene Kan
serene.kan@
wongpartners.com

Chun Hau Ng
chunhau.ng@
wongpartners.com

Effective June 1, 2025, section 12A of the Personal Data Protection Act 2010 ("**PDPA**") requires every data controller and data processor to appoint at least one data protection officer ("**DPO**").

Follow the key considerations below to determine whether you need a DPO.

Subject to the PDPA

Contrary to what one may think, compliance with the PDPA may not be necessary just because you offer goods or services to individuals in Malaysia.

To be subject to the PDPA, you must be: **(a)** established in Malaysia (e.g., a locally incorporated company) and process (e.g., collect, hold, disclose) personal data; or **(b)** using equipment in Malaysia to process personal data for non-transit purposes.

If you are not subject to the PDPA, its DPO obligation does not apply to you. You do not need to read this article any further.

Personal Data > 20,000 Data Subjects

Even if you are subject to the PDPA, the Personal Data Protection Commissioner ("**Commissioner**") has introduced three thresholds, which if triggered result in the DPO obligation being applicable to you.

One such threshold is to consider whether your processing of personal data involves more than 20,000 data subjects (i.e., individuals).

You may or may not meet this threshold just because you have more than 20,000 customers. Some of these customers may be multiple companies with only one individual contact person; conversely, you may have personal data of more than one individual for each company customer.

Be mindful of the retention principle under the PDPA. For example, if you have personal data of employees who have resigned more than 10 years ago, you should consider whether it is still legal to keep such data and action accordingly. This may affect whether you fall within the threshold for the DPO appointment.

Sensitive Personal Data > 10,000 Data Subjects

The DPO obligation is also triggered if you process sensitive personal data (including financial information data) of more than 10,000 data subjects.

Sensitive personal data is essentially a subset of personal data, relating to: **(a)** physical or mental health or condition; **(b)** political opinions; **(c)** religious or similar beliefs; **(d)** commission or alleged commission of offence; or **(e)** biometric data.

Regular and Systematic Monitoring

You will also need to appoint a DPO if your processing of personal data involves activities that require regular and systematic monitoring.

Examples of such regular and systematic monitoring include: **(a)** tracking and profiling data subjects for the purposes of behavioural advertising; **(b)** using algorithms to monitor data subjects' searches and purchases to offer them recommendations on a retail website; **(c)** carrying out activities involving CCTV; **(d)** managing loyalty programme to monitor data subjects' purchase behaviours.

What's Next

If you are subject to the PDPA but do not fulfil any thresholds above, you do not *currently* need a DPO. However, if any of the thresholds are met, you will need a DPO.

As your processing activities may change over time (e.g., expanded business resulting in an increase in the number of employees and individual consumers, new marketing initiatives), you should revisit the thresholds for DPO appointment at appropriate intervals.

If you need to appoint a DPO, do refer to the DPO guidelines and circular issued by the Commissioner for guidance on the requirements and expectations of a DPO, accessible **HERE** and **HERE** respectively.

Practice Area News

Data Breach Notification. Effective June 1, 2025, data controllers may need to notify the Commissioner and the affected data subjects in the event of a personal data breach (i.e., any breach of personal data, loss of personal data, misuse of personal data or unauthorized access of personal data).

The Commissioner has recently issued the relevant guidelines and circular to provide more guidance, accessible **HERE** and **HERE** respectively.

Cybersecurity Service Provider Licence. The extended grace period has ended on February 28, 2025 for cybersecurity service providers to apply for licence under the Cybersecurity Act 2024.

This means that those who provide licensable cybersecurity services i.e., managed security operation centre monitoring service and penetration testing service, without a licence (or at least, an ongoing licence application), have a real risk of committing an offence punishable with fines (up to MYR 500,000) and/or imprisonment (up to 10 years).

Data Processors' Obligations. Effective April 1, 2025, data processors have a direct obligation under the PDPA to comply with the security principle.

This means that data processors may face criminal consequences of fines (up to MYR 1,000,000) and/or imprisonment (up to 3 years), if they fail to take practical steps to protect personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction (which include providing sufficient guarantees on the technical and organizational security measures).

In the Firm

• Awarded Malaysia Trademark Contentious Firm of the Year at 2024 Asia IP Awards

Won the Malaysia Trademark Contentious Firm of the Year at Asia IP's 2024 Awards ceremony held in November 2024.

Asia IP magazine ranks us Tier 1 for Patent Contentious, Patent Prosecution, Trademark Contentious, Trademark Prosecution and Copyright.

• Strongly Ranked Across the IP & Technology Practices by Chambers & Partners and Legal 500

Intellectual Property

- Band 1 by Chambers Asia Pacific
- Tier 1 by Legal 500 Asia Pacific

Technology, Media, Telecoms (TMT)

- Band 2 by Chambers Asia Pacific
- Tier 2 by Legal 500 Asia Pacific

Level 21, The Gardens South Tower, Mid Valley City, Lingkaran Syed Putra, Kuala Lumpur 59200